WE CLAIM

1   1.   A method, comprising:

2   analyzing a transport stream; and

3   preparing the transport stream for processing that bypasses encrypted

4   portions of the transport stream.

1   2.   A method according to Claim 1, wherein analyzing the transport

2   stream includes determining which portions of the transport stream are to pass

3   unencrypted.

1   3.   A method according to Claim 2, wherein determining which portions

2   of the transport stream are to pass unencrypted is executed based on a statistical analysis.

1   4.   A method according to Claim 2, wherein determining which portions

2   of the transport stream are to pass unencrypted is executed dynamically.

1   5.   A method according to Claim 2, wherein determining which portions

2   of the transport stream are to pass unencrypted includes determining a permissible

3   incursion beyond a packet header to gather data for the processing.

1   6.   A method according to Claim 2, wherein determining which portions

2   of the transport stream are to pass unencrypted includes detecting a data packet

3   containing at least a portion of a packetized elementary stream (PES) header.

1   7.   A method according to Claim 2, wherein determining which portions

2   of the transport stream are to pass unencrypted includes detecting bytes of data that are

3   required for processing the transport stream.

1   8.   A method according to Claim 1, wherein preparing the transport

2   stream for processing includes encrypting portions of the transport stream that are not to

3   pass unencrypted.

1   9.   A method according to Claim 1, wherein preparing the transport

2   stream for processing includes encrypting packets containing PES payload data.

1   10.   A method according to Claim 1, wherein preparing the transport

2   stream for processing includes leaving a packet containing a portion of a frame header

3   unencrypted.

1   11.   A method according to Claim 1, wherein preparing the transport

2   stream for processing includes leaving bytes of data unencrypted that are required for

3   processing the transport stream.

1   12.   A method according to Claim 1, wherein preparing the transport

2   stream for processing includes common scrambling packets composed of PES payload

3   data.

1   13.   A method according to Claim 1, wherein preparing the transport

2 stream for processing includes:

3   generating a multiplex-compliant encryption method packet; and

4   inserting the multiplex-compliant encryption method packet into the

5 transport stream.

1   14.   A method according to Claim 13, wherein the encryption method

2 packet identifies an encryption algorithm used in preparing the transport stream for

3 processing, identifies encrypted portions of the transport stream, and provides data for

4 deriving a decryption key.

1   15.   A method according to Claim 13, wherein the encryption method

2 packet identifies an unencrypted portion of the transport stream, a location of the

3 encrypted portion of the unencrypted portion of the transport stream, and a process

4 corresponding to the unencrypted portion of the transport stream.

1   16.   A method according to Claim 13, wherein the encryption method

2 packet is delivered via a private table.

1   17.   A method, comprising:

2   receiving a partially encrypted transport stream; and

3   processing the transport stream in a manner that bypasses encrypted

4 portions of the transport stream.

1   18.   A method according to Claim 17, further comprising:

2   receiving a multiplex-compliant encryption method packet corresponding

3 to the transport stream; and

4   decrypting encrypted portions of the transport stream using a decryption

5 key.

1   19.   A method according to Claim 18, wherein the decryption key is

2 included in the encryption method packet or is received in an out-of-band message.

1   20.   A method according to Claim 17, wherein processing the transport

2 stream includes demultiplexing the transport stream based on unencrypted portions of the

3 transport stream.

1   21.   A method according to Claim 17, wherein processing the transport

2 stream includes indexing payload data contained in the transport stream based on

3 unencrypted portions of the transport stream.

1   22.   A computer-readable medium having one or more instructions that

2 are executable by one or more processors, the one or more instructions causing the one or

3 more processors to:

4   determine which portions of a transport stream are to pass unencrypted for

5 processing that disregards encrypted portions of the transport stream; and

6   prepare the transport stream for the processing.

1   23.   A computer-readable medium according to Claim 22, wherein the

2   one or more instructions to determine which portions of the transport stream are to pass

3   unencrypted cause the one or more processors to leave unencrypted data packets having

4   at least a portion of a PES header.

1   24.   A computer-readable medium according to Claim 22, wherein the

2   one or more instructions to determine which portion of the transport stream are to pass

3   unencrypted cause the one or more processors to leave unencrypted bytes of data required

4   for processing the transport stream.

1   25.   A computer-readable medium according to Claim 22, wherein the

2   one or more instructions to determine which portions of the transport stream are to pass

3   unencrypted cause the one or more processors to leave unencrypted a threshold amount

4   of data beyond packet header data that is relevant for the processing.

1   26.   A computer-readable medium according to Claim 22, wherein the

2   one or more instructions to prepare the transport stream for the processing cause the one

3   or more processors to encrypt portions of the transport stream that are not to pass

4   unencrypted.

1   27.   A computer-readable medium according to Claim 26, wherein the

2   one or more instructions causing the one or more processors to encrypt portions of the

3   transport stream applies an advanced encryption standard (AES)-counter (CTR) mode

4   cipher.

1   28.   A computer-readable medium according to Claim 26, comprising

2 one or more further instructions causing the one or more processors to:

3   generate a multiplex-compliant encryption method packet; and

4   insert the multiplex-compliant encryption method packet into the transport

5 stream.

1   29.   A computer-readable medium according to Claim 22, wherein the

2 encryption method packet identifies an encryption algorithm used to prepare the transport

3 stream for processing, identifies encrypted portions of the transport stream, and provides

4 at least a basis for key to decrypt the encrypted portions of the transport stream.

1   30.   A computer-readable medium according to Claim 22, wherein the

2 encryption method packet identifies an unencrypted portion of the transport stream, a

3 location of the unencrypted portion of the transport stream, and a process associated with

4 the unencrypted portion of the transport stream.

1   31.   A computer-readable medium having one or more instructions that

2 are executable by one or more processors, the one or more instructions causing the one or

3 more processors to:

4   receive a partially encrypted transport stream; and

5   process the transport stream based on unencrypted portions of the transport

6 stream.

1   32.   A computer-readable medium according to Claim 31, comprising

2 one or more further instructions causing the one or more processors to:

3   receive a multiplex-compliant encryption method packet corresponding to

4 the transport stream; and

5   decrypt encrypted portions of the transport stream using an encryption key

6 based in the encryption method packet.

1   33.   A computer-readable medium according to Claim 31, wherein the

2 one or more instructions to process the transport stream cause the one or more processors

3 to demultiplex the transport stream based on unencrypted portions of the transport

4 stream.

1   34.   A computer-readable medium according to Claim 31, wherein the

2 one or more instructions to process the transport stream cause the one or more processors

3 to index payload data contained in the transport stream based on unencrypted portions of

4 the transport stream.

1   35.   An apparatus, comprising:

2   an analyzer to determine which portions of a transport stream are to pass

3 unencrypted for processing that does not incorporate encrypted portions of the transport

4 stream; and

5   a scrambler to encrypt other portions of the transport stream based on the

6 determination.

1   36. An apparatus according to Claim 35, wherein the analyzer is to

2 dynamically determine that a threshold incursion into payload data is to pass unencrypted

3 in order to process the transport stream without removing the encryption from other

4 portions of the transport stream.

1   37. An apparatus according to Claim 35, wherein the analyzer is to

2 determine that a packet containing at least a portion of a PES header is to pass

3 unencrypted.

1   38. An apparatus according to Claim 35, wherein the analyzer is to

2 determine that data arbitrarily disposed throughout PES payload data are to pass

3 unencrypted.

1   39. An apparatus, comprising:

2   means for determining which portions of a transport stream are to pass

3 unencrypted for processing that does not incorporate encrypted portions of the transport

4 stream; and

5   means for encrypting other portions of the transport stream in accordance

6 with the analysis.

1   40. An apparatus according to Claim 39, wherein the means for

2 determining designates a dynamically determined amount of payload data to pass

3 unencrypted in order to process the transport stream without removing the encryption

4 from other portions of the transport stream.